****

**TTTN2423**

**Switching, Routing and Wireless Essentials**

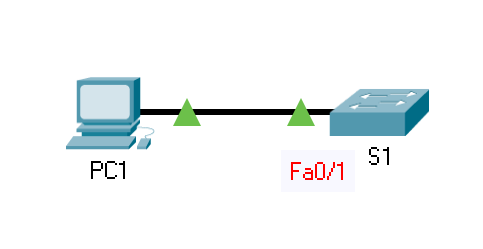
**(CCNA2)**

**Lab 1**

|  |  |
| --- | --- |
| **NAME** | **MOHAMAD SAIFUL NIZAM BIN ABD AZIZ** |
| **NO. MATRIC** | **A179830** |

Packet Tracer - Configure SSH

# Topology



# Addressing Table

| Device | Interface | IP Address | Subnet Mask |
| --- | --- | --- | --- |
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |

Blank Line - no additional information

# Objectives

Part 1: Secure Passwords

Part 2: Encrypt Communications

Part 3: Verify SSH Implementation

# Background

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

# Instructions

## Secure Passwords

* + - 1. Using the command prompt on **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.
      2. Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **S1**.
      3. Show the current configuration and note that the passwords are in plain text. Enter the command that encrypts plain text passwords:

S1(config)# **service password-encryption**

* + - 1. Verify that the passwords are encrypted.

## Encrypt Communications

### Set the IP domain name and generate secure keys.

It is generally not safe to use Telnet, because data is transferred in plain text. Therefore, use SSH whenever it is available.

* + - 1. Configure the domain name to be **netacad.pka**.
      2. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

### Create an SSH user and reconfigure the VTY lines for SSH-only access.

* + - 1. Create an **administrator** user with **cisco** as the secret password.
      2. Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access. Remove the existing vty line password.

### Verify SSH Implementation

* + - 1. Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.
      2. Attempt to log in using SSH. Type **ssh** and press **Enter** without any parameters to reveal the command usage instructions. **Hint**: The **-l** option is the letter “L”, not the number 1.
      3. Upon successful login, enter privileged EXEC mode and save the configuration. If you were unable to successfully access **S1**, toggle the power and begin again at Part 1.

# Reflection Questions

* 1. How did you prevent passwords from being viewed or sent in plaintext?
* by using service password encryption command.
  1. Compare the two methods of remote access used to manage the switch.
* Telnet is insecure because it communicates in plain text, whereas SSH is more secure because it encrypts all data sent between devices, providing security for remote connections.
  1. In Part 2, Step 2b, which command allows you to permit SSH only?
* transport input ssh command.
  1. In Part 2, Step 3c, why were you advised to “toggle the power and begin again at Part 1” if you were not successful in accessing the switch using SSH?
* We need to save the startup configuration in Part 1. We can reconfigure the SSH from the previous saved starting configuration by toggling the switch's power.
  1. Review IP addressing and explain how it is used in this small network.
* The S1 device's IP address is 10.10.10.2, while the PC1 device's IP address is 10.10.10.10. Both use the same 255.255.255.0 subnet mask, indicating that the network can support up to 254 unique hosts. Because PC1 and S1 are on the same network, they don't need a router to communicate.

Type your answers here.

End of document